AF

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
DALE E. GULICK

Serial No.: 09/853,446

Filed: May 11, 2001

For:
RESOURCE SEQUESTER MECHANISM

Examiner: TIM VO

Group Art Unit: 2112

Att'y Docket: 2000.038600

Customer No. 023720

APPEAL BRIEF

CERTIFICATE OF MAILING
37 C.F.R. 1.8

I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date below:

04/08/05 Kathy Llanas
Date Signature

Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant hereby submits this revised Appeal Brief to the Board of Patent Appeals and Interferences in response to the Notification of Non-Compliant Appeal Brief mailed April 4, 2005.

No fees are believed due. However, the Commissioner is authorized to deduct any required fees from **Advanced Micro Devices, Inc.'s Deposit Account 01-0365/TT3759.** In the event the monies in that account are insufficient, the Commissioner is authorized to withdraw funds from Williams, Morgan & Amerson, P.C. Deposit Account No. 50-0786/2000.038600.

I. REAL PARTY IN INTEREST

The present application is owned by Advanced Micro Devices, Inc. The assignment of the present application to Advanced Micro Devices, Inc., is recorded at Reel 011816, Frame 0522.

II. RELATED APPEALS AND INTERFERENCES

Applicant is not aware of any related appeals and/or interferences that might affect the outcome of this proceeding.

III. STATUS OF THE CLAIMS

Claims 1-11 have been withdrawn from consideration. Thus, claims 12-21 are pending in the application. The claims as currently pending are attached as Appendix A. Claims 12-21 stand rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by Wiedemer (U.S. Patent No. 5,155,680).

IV. STATUS OF AMENDMENTS

There were no amendments after the final rejections.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Many conventional computer systems, including personal computers, laptop computers, and the like, implement an x86 operating environment. Privacy, security, and ownership (collectively, PSO) of information stored and/or transmitted by computer systems is becoming critical in an age of Internet-connected computers. The original personal computers were not

designed in anticipation of PSO needs. Consequently, from a hardware point of view, the x86 operating environment provides little for protecting user privacy, providing security for corporate secrets and assets, or protecting the ownership rights of content providers. From a software point of view, the x86 operating environment is equally poor for PSO. The ease of direct access to the hardware through software or simply by opening the cover of the personal computer allows an intruder or thief to compromise most security software and devices. The personal computer's exemplary ease of use only adds to the problems for PSO.

At least in part to address the PSO needs of computer systems, claims 11, 15, 16, and 19 set forth methods of operating a computer system in System Management Mode (SMM). The computer system includes a processor coupled to a memory, to security hardware, and to a first device. For example, Fig. 4 illustrates a block diagram of an embodiment of a portion of an improved version of computer system 100 including security hardware 370 in a south bridge 330, as well as a crypto-processor 305. The south bridge 330 includes the security hardware 370, an interrupt controller (IC) 365, USB interface logic 134C, and the LPC bus interface logic (LPC BIL) 134D. The IC 365 is coupled to the processor 102. The USB interface logic 134C is coupled through an optional USB hub 315 to a biometric device 320 and a smart card reader 325. The LPC bus 118 is coupled to the south bridge 330 through the LPC BIL 134D. The crypto-processor 305 is also coupled to the LPC bus 118. A memory permission table 310 within the Crypto-processor 305 provides address mappings and/or memory range permission information. The memory permission table 310 may be comprised in a non-volatile memory. A BIOS 355, i.e. some memory, preferably read-only memory or flash memory, is coupled to the crypto-processor 305. The security hardware 370 may include both security hardware and secure assets protected

by the security hardware. See Patent Application, page 17, line 15 – page 18, line 3 and Figure 4.

The claimed methods include unlocking security hardware, accessing the first device, locking the security hardware, and calling an SMM exit routine. For example, method 1600F includes the processor loading code instructions into SMM space in the RAM memory, in block 1605. The access locks to the security hardware are opened in block 1615. The processor processes the code instructions from SMM space in the RAM memory, in block 1620. The method 1600F includes accessing the security hardware 370, in block 1630. As the computer system is in SMM and the access locks have been opened, in block 1615, the security hardware is available to most or all of the subsystems of the computer system 100 (or 800), as desired. The method 1600F includes closing the access locks to the security hardware 370, in block 1650. The processor reloads the previous state and continues operating, in block 1665. See Patent Application, page 54, ll. 5-23 and Figure 16F.

As defined in the specification, System Management Mode (SMM) is a mode of operation in the computer system that was implemented to conserve power. The SMM was created for the fourth generation x86 processors. As newer x86 generation processors have appeared, the SMM has become relatively transparent to the operating system. That is, computer systems enter and leave the SMM with little or no impact on the operating system. See Patent Application, page 13, ll. 13-17.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Appellant respectfully requests that the Board review and overturn the single rejection present in this case. The following issue is presented on appeal in this case:

(A) Whether claims 12-21 are anticipated by Wiedemer.

VII. ARGUMENT

A. Claims 12-21 are not anticipated by Wiedemer.

As the Examiner well knows, an anticipating reference by definition must disclose every limitation of the rejected claim in the same relationship to one another as set forth in the claim. *In re Bond*, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990).

Wiedemer is directed to a computer software security and billing system. The Examiner alleges that Wiedemer teaches a method of operating a computer system in System Management Mode. Applicant respectfully disagrees. As stated above and defined in the specification, System Management Mode (SMM) is a mode of operation in the computer system that was implemented to conserve power. Applicant respectfully submits that Wiedemer does not teach or suggest a computer system capable of operating in System Management Mode. In fact, Wiedemer appears to be completely silent with regard to System Management Mode. Accordingly, Applicant submits that Wiedemer fails to teach or suggest calling an SMM exit routine, as set forth in claims 12, 15-16, and 19.

In the FINAL Office Action, the Examiner argues that the preambles of independent claims 12, 15-16, and 19 do not state that "the system management mode is a mode of operation in the computer system that was implemented to conserve power." Thus, the Examiner alleges that Appellant's argument that Wiedemer is completely silent with regard to System

management mode and, in particular, fails to describe or suggest calling a system management mode exit routine, is moot. Appellant respectfully disagrees and notes that there is no statutory requirement terms used in the claims must also be defined in the claims. To the contrary, it is well established that terms used in the claims are to be interpreted in light of the specification and that Appellant is entitled to be his or her own lexicographer. See MPEP §2111.01. Appellant respectfully submits that the term "system management mode" is defined in the specification and thus an explicit definition of this term does not need to be present in the claims.

Appellant respectfully requests that the Examiner's rejections of claims 12-21 be REVERSED.

VIII. CLAIMS APPENDIX

The claims that are the subject of the present appeal – claims 12-21 – are set forth in the attached "Claims Appendix."

IX. EVIDENCE APPENDIX

There is no separate Evidence Appendix for this appeal.

X. RELATED PROCEEDINGS APPENDIX

There is no Related Proceedings Appendix for this appeal.

XI. CONCLUSION

In view of the foregoing, it is respectfully submitted that the Examiner erred in not allowing all claims pending in the present application, claims 12-21, over the prior art of record. The undersigned may be contacted at (713) 934-4052 with respect to any questions, comments or suggestions relating to this appeal.

Respectfully submitted,

Date: 4/8/05

Mark W. Sincell, Ph.D.
Reg. No. 52,226
WILLIAMS, MORGAN & AMERSON
10333 Richmond, Suite 1100
Houston, Texas 77042
(713) 934-7000
(713) 934-7011 (facsimile)

AGENT FOR APPLICANTS

CLAIMS APPENDIX

12. A method of operating a computer system in System Management Mode (SMM), the computer system including a processor coupled to a memory, to security hardware, and to a first device, the method comprising:

unlocking security hardware;

accessing the first device;

locking the security hardware; and

calling an SMM exit routine.

13. The method of claim 12, further comprising:

checking a lock status of the security hardware.

14. The method of claim 12, further comprising:

processing SMM code instructions.

15. A computer system configured to operate in System Management Mode (SMM), the computer system comprising:

means for unlocking security hardware;

means for accessing the first device;

means for locking the security hardware; and

means for calling an SMM exit routine.

16. A computer readable program storage device encoded with instructions that, when executed by a computer system including a processor coupled to a memory, to security hardware, and to a first device, performs a method of operating a computer system in System Management Mode (SMM), the computer system, the method comprising:

unlocking security hardware;

accessing the ~~a~~ first device;

locking the security hardware; and

calling an SMM exit routine.

17. The computer readable program storage device of claim 16, the method further comprising:

checking a lock status of the security hardware.

18. The computer readable program storage device of claim 16 ~~12~~, the method further comprising:

processing SMM code instructions.

19. A method of operating a computer system in System Management Mode (SMM), the computer system including a processor coupled to a memory, to security hardware, and to a first device that is accessible when the security hardware is unlocked and is not accessible when the security hardware is locked, the method comprising:

unlocking security hardware;

accessing the first device;

locking the security hardware; and

calling an SMM exit routine.

20. The method of claim 19, further comprising:

checking a lock status of the security hardware.

21. The method of claim 19, further comprising:

processing SMM code instructions.